WHAT IS CLAIMED IS:

1. A security system for securing data in a computer network comprising:

a plurality of user terminals coupled to the computer network;

a cryptographic device remote from the plurality of user terminals and coupled to the computer network, wherein the cryptographic device includes a computer executable code for authenticating one or more users and verifying that the authenticated user is authorized to assume a role; and

a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user.

2. The system of claim 1, wherein the security device transaction data related to a user is loaded into the cryptographic device when the user requests to operate on a value bearing item.

3. The system of claim 1, wherein the assumed role includes one or more corresponding operations to be performed by the authenticated user.

4. The system of claim 1, wherein the assumed role is a security officer role to initiate a key management function.

5. The system of claim 1, wherein the assumed role is a key custodian role to take possession of shares of keys.

6. The system of claim 1, wherein the assumed role is an administrator role to manage a user access control database.

7. The system of claim 1, wherein the assumed role is an auditor role to manage audit logs.

8. The system of claim 1, wherein the assumed role is a provider role to withdraw from a user account.

9. The system of claim 1, wherein the assumed role is a user role to operate on a VBI.

10. The system of claim 1, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

11. The system of claim 1, wherein the cryptographic device includes a state machine for determining a state corresponding to availability of one or more commands in conjunction with the role.

12. The system of claim 1, wherein the cryptographic device is stateless.

13. The system of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized modification of data.

14. The system of claim 1, wherein the cryptographic device includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions.

15. The system of claim 1, wherein at least one of the user is an enterprise account.

16. The system of claim 1, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

17. The system of claim 2, wherein the value bearing item is a mail piece.

18. The system of claim 17, wherein the postal indicium comprises a digital signature.

19. The system of claim 1, wherein the cryptographic device encrypts validation information according to a user request for printing a VBI.

20. The system of claim 17, wherein the cryptographic device generates data sufficient to print a postal indicium in compliance with postal service regulation on the mail piece.

21. The system of claim 2, wherein the value bearing item is a ticket.

22. The system of claim 2, wherein a bar code is printed on the value bearing item.

23. The system of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

24. The system of claim 1, wherein each security device transaction data includes a private key, a public key, and a public key certificate, wherein the private key is used to sign device

status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

25. The system of claim 1 further comprising at least one more cryptographic device remote from the plurality of user terminals coupled to the computer network, wherein the at least one more cryptographic device includes a computer executable code for authenticating any of the plurality of users.

26. The system of claim 25, wherein the cryptographic device shares a secret with the at least one more cryptographic device.

27. The system of claim 25, wherein one of the plurality of cryptographic devices is a master device and generates a master key set (MKS).

28. The system of claim 27, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device and a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

29. The system of claim 27, wherein the MKS is exported to other cryptographic devices by any cryptographic device.

30. A method for securing data in a computer network having a plurality of user terminals, the method comprising the steps of:

storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of user terminals;

securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals;

storing a plurality of security device transaction data,

wherein each transaction data is related to one of the plurality of users; and

verifying that a user is authorized to assume a role.

31. The method of claim 30 further comprising the step of loading a security device transaction data related to a user into one of the one or more of cryptographic devices when the user requests to operate on a value bearing item.

32. The method of claim 30 further comprising the step of authenticating the identity of each user.

33. The method of claim 30 further comprising the steps of verifying that the user is authorized to perform a corresponding operation based on the assumed role.

34. The method of claim 30, wherein the assumed role is a security officer role and the corresponding command is initiating a key management function.

35. The method of claim 30, wherein the assumed role is a key custodian role to take possession of shares of keys.

36. The method of claim 30, wherein the assumed role is an administrator role to manage a user access control.

37. The method of claim 30, wherein the assumed role is an auditor role to manage audit logs.

38. The method of claim 30, wherein the assumed role is a provider role to authorize increasing credit for a user account.

39. The method of claim 30, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

40. The method of claim 30, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

41. The method of claim 30, further comprising the step of determining a state corresponding to availability of one or more commands in conjunction with the roles.

42. The method of claim 41, wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state.

43. The method of claim 30, further comprising the step of storing data for creating an indicium, account maintenance, and revenue protection.

44. The method of claim 30, further comprising the step of printing a mail piece.

45. The method of claim 44, wherein the mail piece includes a digital signature.

46. The method of claim 44, wherein the mail piece includes a postage amount.

47. The method of claim 44, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

48. The method of claim 30, further comprising the step of printing a ticket.

49. The method of claim 30, further comprising the step of printing a coupon.

50. The method of claim 30, wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

51. The method of claim 30, further comprising the step of using a private key to sign device status responses and the VBI which, in conjunction with a public key certificate, demonstrates that the device and the VBI are authentic.

52. The method of claim 30, further comprising the step of sharing a secret with any of the other devices.

53. The method of claim 30, further comprising the step of generating a master key set (MKS).

54. The method of claim 53, wherein the step of generating the MKS comprises the steps of generating a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

55. The method of claim 54, further comprising the step of generating a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

56. The method of claim 30, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.

57. A cryptographic device for securing data on a computer network comprising:

a processor programmed for authenticating a plurality of users on the computer network for secure processing of a value bearing item;

a memory for storing security device transaction data for ensuring authenticity of a user and that the user is authorized to assume a role, wherein the security device transaction data is related to the one of the plurality of users;

a cryptographic engine for cryptographically protecting data; and

an interface for communicating with the computer network.

58. The cryptographic device of claim 57, wherein the processor is programmed to verify that the identified user is authorized to perform an operation corresponding to an assumed role.

59. The cryptographic device of claim 57, wherein the assumed role is a key custodian role to take possession of shares of keys.

60. The cryptographic device of claim 57, wherein the assumed role is an administrator role to manages a user access control database.

61. The cryptographic device of claim 57, wherein the assumed role is a provider role to authorize increasing credit for a user account.

62. The cryptographic device of claim 57, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

63. The cryptographic device of claim 57 further comprising a stored secret for cryptographically protecting data.

64. The cryptographic device of claim 63, wherein the secret is a password.

65. The cryptographic device of claim 63, wherein the secret is a public/private key pair.

66. The cryptographic device of claim 57, wherein the value bearing item is a postage value including a postal indicium.

67. The cryptographic device of claim 57, wherein the value bearing item is a ticket.

68. The cryptographic device of claim 57, wherein the value bearing item includes a bar code.